SOME SPECIAL FAMILIES OF HYPERELLIPTIC CURVES

TANUSH SHASKA

ABSTRACT. Let $\mathcal{L}_g^G$ denote the locus of hyperelliptic curves of genus g whose automorphism group contains a subgroup isomorphic to G. We study spaces $\mathcal{L}_g^G$ for $G \cong \mathbb{Z}_n, \mathbb{Z}_2 \oplus \mathbb{Z}_n, \mathbb{Z}_2 \oplus A_4$, or $SL_2(3)$. We show that for $G \cong \mathbb{Z}_n, \mathbb{Z}_2 \oplus \mathbb{Z}_n$, the space $\mathcal{L}_g^G$ is a rational variety and find generators of its function field. For $G \cong \mathbb{Z}_2 \oplus A_4, SL_2(3)$ we find a necessary condition in terms of the coefficients, whether or not the curve belongs to $\mathcal{L}_g^G$. Further, we describe algebraically the loci of such curves for $g \leq 12$ and show that for all curves in these loci the field of moduli is a field of definition.

1. INTRODUCTION

One of the most interesting problems in algebraic geometry is to obtain a generalization of the theory of elliptic modular functions to the case of higher genus. In the elliptic case this is done by the so-called *j-invariant* of elliptic curves. In the case of genus $g = 2$, Igusa (1960) gives a complete solution via *absolute invariants* i_1, i_2, i_3 of genus 2 curves; see [6]. Generalizing such results to higher genus is much more difficult due to the existence of non-hyperelliptic curves. However, even restricted to the hyperelliptic moduli $\mathfrak{H}_g$, the problem is still unsolved for $g \geq 3$. In other words, there is no known way of identifying isomorphism classes of hyperelliptic curves of genus $g \geq 3$. In terms of classical invariant theory this means that the field of invariants of binary forms of degree $2g + 2$ is not known for $g \geq 3$.

In previous work we have focused on the loci $\mathcal{L}_g^G$ of hyperelliptic curves with G embedded in the automorphism group. In [5] we introduced a way (via dihedral invariants) of identifying isomorphism classes of genus g hyperelliptic curves with non-hyperelliptic involutions. In this paper we study cases when the automorphism group is isomorphic to one of the following: $\mathbb{Z}_n, \mathbb{Z}_2 \oplus \mathbb{Z}_n, \mathbb{Z}_2 \oplus A_4$, and $SL_2(3)$. This is part of a larger project of the author of finding an algorithm which determines the automorphism group of hyperelliptic curves via their invariants and determining whether the field of moduli is the same as the field of definition; see [11].

The second section covers basic facts on automorphism groups of hyperelliptic curves, Hurwitz spaces, and invariants of binary forms. Let $\mathcal{X}_g$ denote a genus g hyperelliptic curve defined over an algebraically closed field k of characteristic zero, $\mathrm{Aut}(\mathcal{X}_g)$ its automorphism group, and z the hyperelliptic involution of $\mathcal{X}_g$. The group $\overline{\mathrm{Aut}}(\mathcal{X}_g) := \mathrm{Aut}(\mathcal{X}_g)/\langle z \rangle$ is called the *reduced automorphism group* of $\mathcal{X}_g$. In this paper we study hyperelliptic curves with reduced automorphism group isomorphic to a cyclic group $\mathbb{Z}_n$ or A_4. We determine the ramification signature σ of the cover $\psi : \mathcal{X}_g \to \mathbb{P}^1$ with monodromy group $G := \mathrm{Aut}(\mathcal{X}_g)$ (cf. section 2.2 for

Date: This paper has been published by Journal of Algebra and Applications on January 2004.

1991 *Mathematics Subject Classification.* 2000 Mathematics Subject Classification: 14Q05, 14Q15, 14R20, 14D22.

Key words and phrases. Hyperelliptic curves, automorphism groups.

details). Hurwitz spaces are moduli spaces of such covers ψ which we denote by $\mathcal{H}_\sigma$. There is a map

$$\Phi_\sigma : \mathcal{H}_\sigma \to \mathcal{M}_g$$

where $\mathcal{M}_g$ is the moduli space of genus g algebraic curves. We denote by $\mathcal{L}_g^G(\sigma)$ the image $\Phi_\sigma(\mathcal{H}_\sigma)$ in the hyperelliptic locus $\mathfrak{H}_g$. Given a curve $\mathcal{X}_g$ we would like to determine if it belongs to the locus $\mathcal{L}_g^G(\sigma)$ and describe points $\mathfrak{p} \in \mathcal{L}_g^G(\sigma)$. Hence, in section 2.3 we introduce invariants of binary forms.

In section three, we study the case when $\overline{\mathrm{Aut}}(\mathcal{X}_g)$ is a cyclic group $\mathbb{Z}_n$. There are three possible signatures and two types of groups that occur as full automorphism groups, namely $\mathbb{Z}_{2n}$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_n$. We show that in all three cases $\mathcal{L}_g^G$ is a rational δ-dimensional variety and $k(\mathcal{L}_g^G) = k(u_1, \ldots, u_\delta)$ with $\mathfrak{u} := (u_1, \ldots, u_\delta)$ defined in terms of the coefficients of the curve. There is a 1-1 correspondence between nonsingular points of $\mathcal{L}_g^G$ and tuples $\mathfrak{u} = (u_1, \ldots, u_\delta)$.

In section four, we focus on the case when $\overline{\mathrm{Aut}}(\mathcal{X}_g) \cong A_4$. There are six possible signatures of the cover $\psi : \mathcal{X}_g \to \mathbb{P}^1$. Three of these ramifications have $\mathbb{Z}_2 \oplus A_4$ as monodromy group and the other three have $SL_2(3)$. We find equations of these curves in each case. We prove that if $\overline{\mathrm{Aut}}(\mathcal{X}_g) \cong A_4$, then $I_4(\mathcal{X}_g) = 0$ (cf. section 3). This gives a nice necessary condition of checking whether $\mathcal{X}_g$ has automorphism group $\mathbb{Z}_2 \oplus A_4$ or $SL_2(3)$.

In the last section we focus on zero or 1-dimensional subvarieties $\mathcal{L}_g^G$ of $\mathfrak{H}_g$ for $G \cong \mathbb{Z}_2 \oplus A_4, SL_2(3)$. In each case we find explicit equations of such varieties in terms of $GL_2(k)$-invariants of binary forms of degree $2g+2$. This gives an efficient algebraic way of determining if the automorphism group of a genus $g \leq 12$ is $\mathbb{Z}_2 \oplus A_4$ or $SL_2(3)$. Such a method can be easily generalized to higher genus. Further, we show that for each $\mathcal{X}_g \in \mathcal{L}_g^G$, $g \leq 12$, the field of moduli is the same as the field of definition.

Notation: Throughout this paper k denotes an algebraically closed field of characteristic zero, g an integer ≥ 2, and $\mathcal{X}_g$ a hyperelliptic curve of genus g defined over k. $\mathfrak{H}_g$ is the moduli space of hyperelliptic curves defined over k.

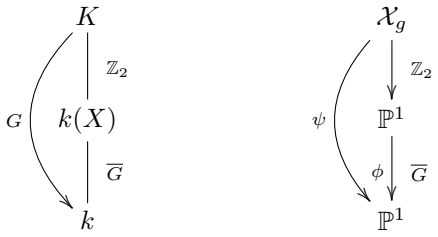
2. Preliminaries

In this section we recall some basic facts about hyperelliptic curves and their automorphisms, Hurwitz spaces, and invariants of binary forms.

2.1. Hyperelliptic curves and their automorphisms.

Let k be an algebraically closed field of characteristic zero and $\mathcal{X}_g$ be a genus g hyperelliptic curve given by the equation $Y^2 = F(X)$, where $\deg(F) = 2g+2$. Denote the function field of $\mathcal{X}_g$ by $K := k(X, Y)$. Then, $k(X)$ is the unique degree 2 genus zero subfield of K. K is a quadratic extension field of $k(X)$ ramified exactly at $d = 2g+2$ places $\alpha_1, \ldots, \alpha_d$ of $k(X)$. The corresponding places of K are called the *Weierstrass points* of K. Let $\mathcal{W} := \{\alpha_1, \ldots, \alpha_d\}$ and $G = Aut(K/k)$. Since $k(X)$ is the only genus 0 subfield of degree 2 of K, then G fixes $k(X)$. Thus, $G_0 := Gal(K/k(X)) = \langle z_0 \rangle$, with $z_0^2 = 1$, is central in G. We call the *reduced automorphism group* of K the group

$\overline{G} := G/G_0$. We illustrate with the following diagram:



By a theorem of Dickson, $\overline{G}$ is isomorphic to one of the following: $\mathbb{Z}_n$, D_n, A_4, S_4, A_5 with branching indices of the corresponding cover $\mathbb{P}^1 \to \mathbb{P}^1/\overline{G}$ given respectively by

$$(n,n),(2,2,n),(2,3,3),(2,4,4),(2,3,5).$$

We focus on cases $\overline{G} \cong \mathbb{Z}_n, A_4$, other cases are intended to be studied in [13].

2.2. **Hurwitz spaces of covers $\psi : \mathcal{X}_g \to \mathbb{P}^1$.** Let $\mathcal{M}_g$ be the moduli space of curves of genus $g \geq 2$ and $\mathbb{P}^1 = \mathbb{P}^1(k)$ the Riemann sphere. Let $\phi : \mathcal{X}_g \to \mathbb{P}^1$ be a degree n covering with r branch points. By covering space theory, there is a tuple $(\sigma_1, \ldots, \sigma_r)$ in S_n such that $\sigma_1 \cdots \sigma_r = 1$ and $G :=< \sigma_1, \ldots, \sigma_r >$ is a transitive group in S_n. We call such a tuple the *signature* of ϕ. We say that a permutation is of type n^p if it is a product of p disjoint n-cycles.

Conversely, let $\sigma := (\sigma_1, \ldots, \sigma_r)$ be a tuple in S_n such that $\sigma_1 \cdots \sigma_r = 1$ and $G :=< \sigma_1, \ldots, \sigma_r >$ is a transitive group in S_n. We say that a cover $\phi : \mathcal{X} \to \mathbb{P}^1$ of degree n is of type σ if it has σ as signature. The genus g of $\mathcal{X}$ depends only on σ (Riemann-Hurwitz formula). Let $\mathcal{H}_\sigma$ be the set of pairs $([f], (p_1, \ldots, p_r))$, where $[f]$ is an equivalence class of covers of type σ, and $p_1, \ldots, p_r$ is an ordering of the branch points of ϕ. The *Hurwitz space* $\mathcal{H}_\sigma$ is a quasiprojective variety; see [3]. We have a morphism

$$\Phi_\sigma : \mathcal{H}_\sigma \to \mathcal{M}_g$$

mapping $([f], (p_1, \ldots, p_r))$ to the class $[\mathcal{X}]$ in the moduli space $\mathcal{M}_g$. Each component of $\mathcal{H}_\sigma$ has the same image in $\mathcal{M}_g$.

We denote by $C := (C_1, \ldots, C_r)$, where C_i is the conjugacy class of σ_i in G. The set of Nielsen classes $\mathcal{N}(G, C)$ is

$$\mathcal{N}(G,C) := \{(\sigma_1, \ldots, \sigma_r) \mid \sigma_i \in C_i,\, G =< \sigma_1, \ldots, \sigma_r >,\ \sigma_1 \cdots \sigma_r = 1\}$$

Fix a base point $\lambda_0 \in \mathbb{P}^1 \setminus S$ where S is the set of branch points. Then $\pi_1(\mathbb{P}^1 \setminus S)$ is generated by homotopy classes of loops $\gamma_1, \ldots, \gamma_r$. The braid group acts on $\mathcal{N}(G, C)$ as

$$[\gamma_i] : \quad (\sigma_1, \ldots, \sigma_r) \to (\sigma_1, \ldots, \sigma_{i-1}, \sigma_i \sigma_{i+1} \sigma_i^{-1}, \sigma_i, \sigma_{i+2}, \ldots, \sigma_r)$$

The orbits of this action are called the *braid orbits* and correspond to the irreducible components of $\mathcal{H}(G, C) := \mathcal{H}_\sigma$.

Lemma 2.1. *Let $\mathcal{X}_g$ be a genus $g \geq 2$ hyperelliptic curve with $\overline{G} := \mathbb{Z}_n, A_4$. Then, $G := Aut(\mathcal{X}_g)$, the dimension δ of $\mathcal{L}_G^\sigma$, the signature σ, and the number of involutions $i(G)$ of G are as follows:*

Proof. The proof is elementary and follows from results in [2]. □

Case	G	$\overline{G}$	$\delta = dim(\mathcal{L}_G^\sigma)$	$\delta \neq$	$\sigma = (\sigma_1, \ldots, \sigma_r)$	*i(G)*
1	$\mathbb{Z}_2 \oplus \mathbb{Z}_n$		$\frac{2g+2}{n} - 1$	$\delta \neq 0, 1$	$(n^2, n^2, 2^n, \ldots, 2^n)$	*3*
2	$\mathbb{Z}_{2n}$	$\mathbb{Z}_n$	$\frac{2g+1}{n} - 1$		$(n^2, 2n, 2^n, \ldots, 2^n)$	*1*
3	$\mathbb{Z}_{2n}$		$\frac{2g}{n} - 1$	$\delta \neq 0, 1$	$(2n, 2n, 2^n, \ldots, 2^n)$	*1*
4	$\mathbb{Z}_2 \oplus A_4$		$\frac{g+1}{6}$		$(3^8, 3^8, 2^{12}, \ldots, 2^{12})$	
5	$\mathbb{Z}_2 \oplus A_4$		$\frac{g-1}{6}$		$(3^8, 6^4, 2^{12}, \ldots, 2^{12})$	*7*
6	$\mathbb{Z}_2 \oplus A_4$	A_4	$\frac{g-3}{6}$	$\delta \neq 0$	$(6^4, 6^4, 2^{12}, \ldots, 2^{12})$	
7	$SL_2(3)$		$\frac{g-2}{6}$	$\delta \neq 0$	$(4^6, 3^8, 3^8, 2^{12}, \ldots, 2^{12})$	
8	$SL_2(3)$		$\frac{g-4}{6}$		$(4^6, 3^8, 6^4, 2^{12}, \ldots, 2^{12})$	*1*
9	$SL_2(3)$		$\frac{g-6}{6}$	$\delta \neq 0$	$(4^6, 6^4, 6^4, 2^{12}, \ldots, 2^{12})$	

TABLE 1. Hyperelliptic curves with reduced automorphism group $\mathbb{Z}_n, A_4$

Let $G := \mathbb{Z}_2 \oplus A_4, SL_2(3)$. Denote by $\mathcal{H}_G^g$ the Hurwitz space $\mathcal{H}(G, C)$ of covers given in Table 1. Spaces $\mathcal{H}_G^g$ are irreducible. To show this we have to show that there is only one braid orbit. By applying the braid action one can assume that the signature is given as $\sigma = (\sigma_1, \sigma_2, \sigma_3, \alpha, \ldots, \alpha)$ where $\sigma_1, \sigma_2, \sigma_3$ are as in Table 1, and α is an involution. Thus, we are looking for 4-tuples $(\sigma_1, \sigma_2, \sigma_3, \alpha)$ or 3-tuples $(\sigma_1, \sigma_2, \sigma_3)$, depends whether r is even or odd, which are transitive in S_{24} and generate G. A computer search would show that there is only such braid orbit. For $r = 4$ these spaces are genus zero curves as can be shown by a direct computation. In section 5 we will describe these spaces algebraically.

Example 2.1. *Let $g = 5$. Then, $\mathcal{H}_G^5$ has genus 0. There are 6 Nielsen classes. One of them is $\sigma = (\alpha, \alpha, \beta, \beta^{-1})$, where α, β are as below:*

$$\alpha = (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)(13,14)(15,16)(17,18)(19,20)(21,22)(23,24),$$
$$\beta = (1,2,3)(4,5,6)(7,8,9)(10,11,12)(13,14,15)(16,17,18)(19,20,21)(22,23,24).$$

Remark 2.1. *An interesting problem would be to decide if $\Phi_\sigma(\mathcal{H}_\sigma) \subset \mathfrak{H}_g$? In other words, are there any genus g non-hyperelliptic curves $\mathcal{Y}_g$ such that there is a cover $\psi : \mathcal{Y}_g \to \mathbb{P}^1$ with signature as in Table 1.*

For the rest of this paper $\mathcal{L}_g^G(\sigma)$ is denoted by $\mathcal{L}_g^G$, since for each genus g there is exactly one signature σ.

2.3. **Invariants of Binary Forms.** In this section we define the action of $GL_2(k)$ on binary forms and discuss the basic notions of their invariants. Let $k[X, Z]$ be the polynomial ring in two variables and let V_d denote the $(d+1)$-dimensional subspace of $k[X, Z]$ consisting of homogeneous polynomials.

$$f(X, Z) = a_0 X^d + a_1 X^{d-1} Z + \ldots + a_d Z^d \tag{1}$$

of degree d. Elements in V_d are called *binary forms* of degree d. We let $GL_2(k)$ act as a group of automorphisms on $k[X, Z]$ as follows:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k), \text{ then } \quad M \begin{pmatrix} X \\ Z \end{pmatrix} = \begin{pmatrix} aX + bZ \\ cX + dZ \end{pmatrix} \tag{2}$$

This action of $GL_2(k)$ leaves V_d invariant and acts irreducibly on V_d.

Remark 2.2. *It is well known that $SL_2(k)$ leaves a bilinear form (unique up to scalar multiples) on V_d invariant. This form is symmetric if d is even and skew symmetric if d is odd.*

Let A_0, A_1, ... , A_d be coordinate functions on V_d. Then the coordinate ring of V_d can be identified with $k[A_0, ..., A_d]$. For $I \in k[A_0, ..., A_d]$ and $M \in GL_2(k)$, define $I^M \in k[A_0, ..., A_d]$ as follows

$$I^M(f) := I(M(f)) \tag{3}$$

for all $f \in V_d$. Then $I^{MN} = (I^M)^N$ and Eq. (3) defines an action of $GL_2(k)$ on $k[A_0, ..., A_d]$. A homogeneous polynomial $I \in k[A_0, \ldots, A_d, X, Z]$ is called a *covariant* of index s if

$$I^M(f) = \delta^s I(f),$$

where $\delta = \det(M)$. The homogeneous degree in $a_1, \ldots, a_n$ is called the *degree* of I, and the homogeneous degree in X, Z is called the *order* of I. A covariant of order zero is called *invariant*. An invariant is a $SL_2(k)$-invariant on V_d.

We will use the symbolic method of classical theory to construct covariants of binary forms. Let

$$f(X,Z) := \sum_{i=0}^{n} \binom{n}{i} a_i X^{n-i} Z^i, \quad \textit{and} \quad g(X,Z) := \sum_{i=0}^{m} \binom{m}{i} b_i X^{n-i} Z^i$$

be binary forms of degree n and m respectively with coefficients in k. We define the **r-transvection**

$$(f,g)^r := \frac{(m-r)!\,(n-r)!}{n!\,m!} \sum_{k=0}^{r} (-1)^k \binom{r}{k} \cdot \frac{\partial^r f}{\partial X^{r-k}\,\partial Z^k} \cdot \frac{\partial^r g}{\partial X^k\,\partial Z^{r-k}}$$

It is a homogeneous polynomial in $k[X, Z]$ and therefore a covariant of order $m + n - 2r$ and degree 2. In general, the r-transvection of two covariants of order m, n (resp., degree p, q) is a covariant of order $m + n - 2r$ (resp., degree $p + q$).

For the rest of this paper $F(X, Z)$ denotes a binary form of order $d := 2g + 2$ as below

$$F(X,Z) = \sum_{i=0}^{d} a_i X^i Z^{d-i} = \sum_{i=0}^{d} \binom{n}{i} b_i X^i Z^{n-i} \tag{4}$$

where $b_i = \frac{(n-i)!\;i!}{n!} \cdot a_i$, for $i = 0, \ldots, d$. We denote invariants (resp., covariants) of binary forms by I_s (resp., J_s) where the subscript s denotes the degree (resp., the order). We define the following covariants and invariants:

$$\begin{aligned}
&I_2 := (F,F)^d, && J_{4j} := (F,F)^{d-2j},\ j = 1, \ldots, g,\\
&I_4 := (J_4, J_4)^4, && I_4' := (J_8, J_8)^8,\\
&I_6 := ((F,J_4)^4, (F,J_4)^4)^{d-4}, && I_6' := ((F,J_8)^8, (F,J_8)^8)^{d-8},\\
&I_6^* := ((F,J_{12})^{12}, (F,J_{12})^{12})^{d-12}, && I_3 := (F,J_d)^d,\\
&M := ((F,J_4)^4, (F,J_8)^8)^{d-10}, && I_{12} := (M,M)^8
\end{aligned} \tag{5}$$

Absolute invariants are called $GL_2(k)$-invariants. We define the following absolute invariants:

$$i_1 := \frac{I_4'}{I_2^2},\ i_2 := \frac{I_3^2}{I_2^3},\ i_3 := \frac{I_6^*}{I_2^3},\ j_1 := \frac{I_6^{'}}{I_3^2},\ j_2 := \frac{I_6}{I_3^2},\ s_1 := \frac{I_6^2}{I_{12}},\ s_2 := \frac{(I_6^{'})^2}{I_{12}}$$

$$\mathfrak{v}_1 := \frac{I_6}{I_6^*},\ \mathfrak{v}_2 := \frac{(I_4')^3}{I_3^4},\ \mathfrak{v}_3 := \frac{I_6}{I_6'},\ \mathfrak{v}_4 := \frac{(I_6^*)^2}{I_4^3}.$$

In the case $g = 10$ and $I_{12} = 0$ we define

$$\begin{aligned} I_6^\star &:= ((F, J_{16})^{16}, (F, J_{16})^{16})^{d-16}), \\ S &:= (J_{12}, J_{16})^{12}, \\ I_{12}^* &:= (\,(J_{16}, S)^4,\, (J_{16}, S)^4\,)^{12} \end{aligned} \tag{6}$$

and

$$\mathfrak{v}_5 := \frac{I_6^\star}{I_{12}^*}.$$

For a given curve $\mathcal{X}_g$ we denote by $I(\mathcal{X}_g)$ or $i(\mathcal{X}_g)$ the corresponding invariants.

Remark 2.3. *We will only perform computations on subvarieties $\mathcal{L}_g^G \subset \mathfrak{H}_g$ of dimension $\delta \leq 1$, hence don't need other absolute invariants.*

3. The reduced automorphism group is cyclic

Let $\overline{\mathrm{Aut}}(\mathcal{X}_g) \cong \mathbb{Z}_n$. Then, $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ has signature (n, n). We identify the branch points of ϕ with $0, \infty$ and the ramified points in their fibers by $0, \infty$ respectively. Hence, $\phi(X) = X^n$. We denote by $V := \phi^{-1}(0) \cup \phi^{-1}(\infty)$. In this section e_t denotes the t-th root of unity, G and δ are as in first three cases of Table 1.

Case 1: If $V \cap \mathcal{W} = \emptyset$, then $n \,|\, 2g+2$ and the equation of the curve is

$$Y^2 = \prod_{i=1}^{t} (X^n - q_i)$$

where q_i's are the branch points of $\psi : \mathcal{X}_g \to \mathbb{P}^1$ not in $\{0, \infty\}$ and $t = \frac{2g+2}{n}$. Let $a_1, \ldots, a_t$ denote the symmetric polynomials in $q_1, \ldots, q_t$. Further we can take $q_1 \ldots q_t = 1$. Hence the equation of the curves is

$$Y^2 = X^{2g+2} + a_1 X^{n\,(t-1)} + \cdots + a_i X^{n\,(t-i)} + \cdots + a_\delta X^n + 1. \tag{7}$$

We need to determine to what extent the normalization above determines the coordinate X. Let γ generate $\mathbb{Z}_n$. Then, $\gamma(X) = e_n X$. This condition determines the coordinate X up to a coordinate change by some $\alpha \in PGL_2(k)$ centralizing γ. Such α satisfies $\alpha(X) = mX$ or $\alpha(X) = \frac{m}{X}$, $m \in k \setminus \{0\}$. The additional condition $(-1)^t q_1 \cdot \cdots q_t = 1$ forces

$$(-1)^t\, \gamma(q_1) \ldots \gamma(q_t) = 1.$$

Hence, $m^t = 1$. So X is determined up to a coordinate change by the subgroup $H \cong D_{2t}$ of $PGL_2(k)$ generated by $\tau_1 : X \to \varepsilon_t X$, $\tau_2 : X \to \frac{1}{X}$, where ε_t is a primitive t-th root of unity.

Case 2: If $|V \cap \mathcal{W}| = 1$ then 0 or ∞ is a Weierstrass point. Then, $n \,|\, 2g+1$ and the equation of the curve is

$$Y^2 = \prod_{i=1}^{t} (X^n - q_i)$$

where q_i's are the branch points of $\psi : \mathcal{X}_g \to \mathbb{P}^1$ and $t = \frac{2g+1}{n}$. Hence the equation of the curve is

$$Y^2 = X^{2g+1} + a_1 X^{n\,(t-1)} + \cdots + a_\delta X^n + 1 \tag{8}$$

Then X is determined up to a coordinate change by the subgroup $H := \langle \tau_1, \tau_2 \rangle$ of $PGL_2(k)$ such that $\tau_1 : X \to \varepsilon_t X$, $\tau_2 : X \to \frac{1}{X}$.

Case 3: If $|V \cap \mathcal{W}| = 2$ then $n \,|\, 2g$ and the curve has equation

$$Y^2 = X(X^{nt} + a_1 X^{n(t-1)} + \cdots + a_\delta X^n + 1) \tag{9}$$

where $t = \frac{2g}{n}$. Then X is determined up to a coordinate change by the subgroup $H := \langle \tau_1, \tau_2 \rangle$ of $PGL_2(k)$ such that $\tau : X \to \varepsilon_t X$, $\tau_2 : X \to \frac{1}{X}$.

Now we consider all three cases. H acts on $k(a_1, \ldots, a_\delta)$ as follows:

$$\begin{aligned} \tau_1 : &\qquad a_i \to \varepsilon^{d-ni} a_i, &&for \quad i = 1, \ldots, \delta \\ \tau_2 : &\qquad a_i \to a_{t-i}, &&for \quad i = 1, \ldots, [\frac{\delta+1}{2}] \end{aligned}$$

Thus, the fixed field $k(a_1, \ldots, a_\delta)^H$ is the same as the function field of the variety $\mathcal{L}_g^G$. We summarize in the following:

Lemma 3.1. $k(\mathcal{L}_g^G) = k(a_1, \ldots, a_\delta)^H$.

The following

$$u_i := a_1^{t-i}\, a_i \,+\, a_\delta^{t-i}\, a_{t-i}, \quad for \quad 1 \le i \le \delta \tag{10}$$

are called *dihedral invariants* for the genus g and the tuple

$$\mathfrak{u} := (u_1, \ldots, u_\delta)$$

is called the *tuple of dihedral invariants*. It can be checked that $\mathfrak{u} = 0$ if and only if $a_1 = a_\delta = 0$. In this case replacing a_1, a_δ by $a_2, a_{\delta-1}$ in the formula above would give new invariants. We would focus in the case that $\mathfrak{u} \neq 0$, as the other cases are simpler. The next theorem shows that the dihedral invariants generate $k(\mathcal{L}_g^G)$.

Theorem 3.1. *Let $\mathcal{L}_g^G$ be as in cases 1, 2, 3, of Lemma 2.1. and $\delta = \dim(\mathcal{L}_g^G)$. Then, $k(\mathcal{L}_g^G) = k(\mathfrak{u}_1, \ldots, \mathfrak{u}_\delta)$.*

Proof. The dihedral invariants are fixed by the H-action. Let $\mathfrak{u} = (u_1, \ldots, u_\delta)$ be the δ-tuple of dihedral invariants. Hence, $k(\mathfrak{u}) \subset k(\mathcal{L}_g^G)$. Thus, it is enough to show that $[k(a_1, \ldots a_\delta) : k(\mathfrak{u})] = 2t$. For each $2 \le i \le \delta - 1$ we have

$$\begin{gathered} a_1^{\delta-i+1} a_i + a_\delta^{\delta-i+1} a_{\delta-i+1} = u_i \\ a_1^i a_{\delta-i+1} + a_\delta^i a_i = u_{\delta-i+1} \end{gathered}$$

giving $a_i,\ a_{t-i} \in k(\mathfrak{u}, a_1, a_\delta)$. Then, the extension $k(a_1, \ldots, a_\delta)/k(u_1, \ldots, u_\delta)$ has equation

$$2^t\, a_g^{2t} - 2^t\, u_1\, a_\delta^t + u_{t-1}^t = 0 \tag{11}$$

This completes the proof.

□

Remark 3.1. *If $n = 2$ then $G = V_4$. Then $\mathcal{L}_g^G = \mathcal{L}_g$ where $\mathcal{L}_g$ is the locus of hyperelliptic curves with extra involutions; see [5]. A nice necessary and sufficient condition is found in [11] in terms of the dihedral invariants for a curve to have more then three involutions in the reduced automorphism group. More precisely, for such curves the relation $2^{g-1}u_1^2 - u_g^{g+1} = 0$ holds.*

4. The reduced automorphism group is isomorphic to A_4

In this section we study genus g hyperelliptic curves $\mathcal{X}_g$ with $\overline{\mathrm{Aut}}(\mathcal{X}_g) \cong A_4$. Thus, A_4 is the monodromy group of a cover $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ with signature $\bar{\sigma} := (\sigma_1, \sigma_2, \sigma_3)$ of type $(2^6, 3^4, 3^4)$; see Table 1. We denote by q_1, q_2, q_3 the corresponding branch points of ϕ. Let S be the set of branch points of $\psi : \mathcal{X}_g \to \mathbb{P}^1$. Clearly $q_1, q_2, q_3 \in S$. As above $\mathcal{W}$ denotes the images in $\mathbb{P}^1$ of Weierstrass points of $\mathcal{X}_g$ and $V := \cup_{i=1}^3 \phi^{-1}(q_i)$.

Lemma 4.1. *Let $V, \mathcal{W}$ be as above and $g \neq 2, 3, 6$. Then the following hold:*

i) if $|V \cap \mathcal{W}| = 0, 4, 8$, then $Aut(\mathcal{X}_g) \cong \mathbb{Z}_2 \oplus A_4$ and $g \equiv -1, 1, 3 \mod 6$ respectively,

ii) if $|V \cap \mathcal{W}| = 6, 10, 14$, then $Aut(\mathcal{X}_g) \cong SL_2(3)$ and $g \equiv 2, 4, 0 \mod 6$ respectively.

Proof. Assume that $|V \cap \mathcal{W}| = 0$. Then, $\phi(w_i)$ are branch points of ϕ. By Riemann-Hurwitz formula $2g+2 \equiv 0 \mod 12$. Then, $g \equiv -1 \mod 6$. The number of branch points of $\psi : \mathcal{X}_g \to \mathbb{P}^1$ is $r = 3 + \frac{g+1}{6}$. If $|V \cap \mathcal{W}| = 4$ then either $\phi^{-1}(q_2) \subset \mathcal{W}$ or $\phi^{-1}(q_3) \subset \mathcal{W}$. Hence, $2g - 2 \equiv 0 \mod 12$ or $g \equiv 1 \mod 6$. If $|V \cap \mathcal{W}| = 8$ then $\phi^{-1}(q_i) \subset \mathcal{W}$ for $i = 2, 3$. Thus, $2g - 6 \equiv 0 \mod 12$ or $g \equiv 3 \mod 6$. In all cases σ_1 lifts to a non hyperelliptic involution in G. Hence G has more then one involution. Hence, $\mathrm{Aut}(\mathcal{X}_g) \cong \mathbb{Z}_2 \oplus A_4$.

If $|V \cap \mathcal{W}| = 6, 10, 14$ then $\phi^{-1}(q_1) \subset \mathcal{W}$, $\phi^{-1}(q_i) \subset \mathcal{W}$ for $i = 1, 2$, $\phi^{-1}(q_i) \subset \mathcal{W}$ for $i = 1, 2, 3$ respectively. Thus, $g \equiv 2, 4, 0 \mod 6$. In all cases σ_1 lifts to an element of order 4 in $\mathrm{Aut}(\mathcal{X}_g)$. Thus, $\mathrm{Aut}(\mathcal{X}_g)$ has only the hyperelliptic involution. Hence, $\mathrm{Aut}(\mathcal{X}_g) \cong SL_2(3)$. □

Remark 4.1. *When $G \cong \mathbb{Z}_2 \oplus A_4$ then the curve has seven involutions as seen in Table 1. Thus, those curves belong to the locus $\mathcal{L}_g$ of curves with extra involutions studied in [5].*

Let $\phi : P^1 \to \mathbb{P}^1$ be as above with monodromy group A_4. Then, the signature is $\sigma = (\sigma_1, \sigma_2, \sigma_3)$, where σ_1 is an involution and σ_2, σ_3 are elements of order 3 in S_{12}. We choose branch points $q_1 = \infty$, $q_2 = 6i\sqrt{3}$, and $q_3 = -6i\sqrt{3}$, where $i^2 = -1$. We choose a coordinate X in $\mathbb{P}^1$ such that $\phi(0) = \phi(\infty) = \phi(1) = \infty$. Solving the corresponding system of equations we find that

$$\phi(X) = \frac{X^{12} - 33X^8 - 33X^4 + 1}{X^2(X^4 - 1)^2}.$$

Thus, the points in the fiber of q_1, q_2, q_3 are the roots of the following polynomials:

$$\begin{aligned} R(X) &:= X(X^4 - 1), \\ S(X) &:= X^4 - 2i\sqrt{3}X^2 + 1, \\ T(X) &:= X^4 + 2i\sqrt{3}X^2 + 1. \end{aligned}$$

Let $\lambda_i \in \mathbb{P}^1 \setminus S$ be a branch point of the cover $\psi : \mathcal{X}_g \to \mathbb{P}^1$. Thus, $\lambda_i^2 + 108 \neq 0$. Then points of $\phi^{-1}(\lambda_i)$ are roots of the polynomial

$$G_i(X) = X^{12} - \lambda_i X^{10} - 33X^8 + 2\lambda_i X^6 - 33X^4 - \lambda_i X^2 + 1. \tag{12}$$

$G_i(X)$ has distinct roots for $\lambda_i^2 \neq 108$.

Remark 4.2. *The rational function $\phi(x)$ generates the fixed field of A_4 in $k(X)$. It was known to Klein and has appeared many times in the literature since. Indeed,*

we picked the coordinate X in $\mathbb{P}^1$ such that our expression of $\phi(X)$ would be in this form.

We now can compute the equation of the curve in all cases 4-8 of Table 1. If $\mathcal{W} \cap V = \emptyset$ then the equation of the curve is $Y^2 = G(X)$ where

$$G(X) = \prod_{i=1}^{\delta} G_{\lambda_i}(X)$$

and $\delta = \frac{g+1}{6}$; see Lemma (4.1). If $\phi^{-1}(q_i) \subset \mathcal{W}$ then the polynomial corresponding to q_i multiplies $G(X)$. Hence, we have the following:

Lemma 4.2. *The equations of the curve $\mathcal{X}_g$ in each case are given by:*

G	δ	Equation $Y^2 =$
$\mathbb{Z}_2 \oplus A_4$	$\frac{g+1}{6}$	$G(X)$
$\mathbb{Z}_2 \oplus A_4$	$\frac{g-1}{6}$	$(X^4 + 2i\sqrt{3}X^2 + 1) \cdot G(X)$
$\mathbb{Z}_2 \oplus A_4$	$\frac{g-3}{6}$	$(X^8 + 14X^4 + 1) \cdot G(X)$
$SL_2(3)$	$\frac{g-2}{6}$	$X(X^4 - 1) \cdot G(X)$
$SL_2(3)$	$\frac{g-4}{6}$	$X(X^4 - 1)(X^4 + 2i\sqrt{3}X^2 + 1) \cdot G(X)$
$SL_2(3)$	$\frac{g-6}{6}$	$X(X^4 - 1)(X^8 + 14X^4 + 1) \cdot G(X)$

TABLE 2. Hyperelliptic curves $\mathcal{X}_g$ with $\overline{\mathrm{Aut}}(\mathcal{X}_g)$ isomorphic to A_4.

Remark 4.3. *From the group theory viewpoint we have $\sigma_1(X) : X \to -X$ and $\sigma_2 : X \to \frac{X-i}{X+i}$, where $i^2 = -1$. It is easily checked that σ_1, σ_2 generate A_4. Let $t \in \mathcal{W}$. The orbit of A_4 in $\mathcal{W}$ is*

$$t, \frac{t-i}{t+i}, -i\frac{t+1}{t-1}, \frac{t+i}{t-i}, -i\frac{t-1}{t+1}, \frac{1}{t}, -t, -\frac{t-i}{t+i}, i\frac{t+1}{t-1}, -\frac{t+i}{t-i}, i\frac{t-1}{t+1}, -\frac{1}{t}$$

We label these points as $\alpha_1, \ldots, \alpha_{12}$. Then, the polynomial $G_i(X) = \prod_{i=1}^{12}(x - \alpha_i)$ is the polynomial in (12) where $\lambda_i = \frac{t^{12} - 33t^8 - 33t^4 + 1}{t^2(t^4-1)^2}$.

Let $\mathcal{X}_g$ be a given curve. When does $\mathcal{X}_g$ belong to one of the above cases? Can we find a condition on the coefficients of the curve such that $|\mathrm{Aut}(\mathcal{X}_g)| = 24$? The following lemma determines a necessary condition that $|\mathrm{Aut}(\mathcal{X}_g)| = 24$.

Lemma 4.3. *Let $\mathcal{X}_g$ be a curve with $\overline{Aut}(\mathcal{X}_g) \cong A_4$. Then $I_4(\mathcal{X}_g) = 0$.*

Proof. Computationally we show that $I_4(G_i) = 0$. Then, lemma follows from properties of transvections.

□

5. Applications, subvarieties $\mathcal{L}_g^G$ of dimension $\delta \leq 1$

In this section, we study in more detail subvarieties $\mathcal{L}_g^G$ in Table 1, of dimension $\delta \leq 1$ when $G \cong \mathbb{Z}_2 \oplus A_4, SL_2(3)$. We determine invariants which classify isomorphism classes of such curves. These invariants are used to prove that the field of

definition of such curves is the same as the field of moduli. For curves with automorphism group $\mathbb{Z}_2 \oplus A_4$ this is a consequence of Theorem 4.2., in [11] and holds for any genus. However, no results are know for curves with automorphism group $SL_2(3)$. Proposition 5.2., addresses this question for $g \leq 12$. From equations in Table 2 we get the following lemma:

Lemma 5.1. *Let $\mathcal{X}_g$ be a hyperelliptic curve of genus $g \leq 12$. Then.*
i) if $g = 4$ then $I_2 = I_4 = I_4^{'} = I_6^{'} = 0$
ii) if $g = 5, 9, 12$ then $I_4 = I_6 = 0$
iii) if $g = 7, 10$ then $I_2 = I_4 = I_4^{'} = I_6^{*} = 0$
iv) if $g = 8$ then $I_4 = 0$.

Then we define $\mathfrak{p}(\mathcal{X}_g)$ as follows:

$$\mathfrak{p}(\mathcal{X}_g) := (\mathfrak{p}_1, \mathfrak{p}_2) = \begin{cases} \mathfrak{v}_1, & \text{if } g = 4, \\ (i_1, i_2), & \text{if } g = 5, 9, \text{ and } I_2 \neq 0 \\ \mathfrak{v}_2, & \text{if } g = 5, 9, \text{ and } I_2 = 0 \\ (j_1, j_2), & \text{if } g = 7, \text{ and } I_3 \neq 0 \\ \mathfrak{v}_3, & \text{if } g = 7, \text{ and } I_3 = 0 \\ (i_1, i_3), & \text{if } g = 8, 12, \text{ and } I_2 \neq 0 \\ \mathfrak{v}_4, & \text{if } g = 8, 12, \text{ and } I_2 = 0 \\ (s_2, s_1), & \text{if } g = 10, \text{ and } I_{12} \neq 0 \\ \mathfrak{v}_5, & \text{if } g = 10, \text{ and } I_{12} = 0 \end{cases}$$

The following theorem uses these invariants to parametrize spaces $\mathcal{L}_g^G$, where $G \cong \mathbb{Z}_2 \oplus A_4, SL_2(3)$. In the case that $\delta = 1$ these spaces are genus 0 curves. This can be proved via Hurwitz spaces, as noticed in Section 2. However, the next theorem provides an algebraic description of such spaces.

Theorem 5.1. *Let $\mathcal{X}_g, \mathcal{X}_g^{'}$ be genus $g \leq 12$ hyperelliptic curves with automorphism group $\mathbb{Z}_2 \oplus A_4, SL_2(3)$. Then, $\mathcal{X}_g \cong \mathcal{X}_g^{'}$ if and only if $\mathfrak{p}(\mathcal{X}_g) = \mathfrak{p}(\mathcal{X}_g^{'})$. Moreover, the*

moduli space $\mathcal{L}_g^G$ *can be parametrized as follows:*

$$\mathcal{L}_5^G: \quad \mathfrak{p} = \left(\tfrac{49}{3630}\,\tfrac{(5\theta-484)^2}{(5\theta+924)^2},\ \tfrac{10}{27951}\,\tfrac{\theta\,(5\theta+30492)^2}{(5\theta+924)^3}\right),\ \textit{and}\ \mathfrak{p} = \tfrac{3^7\cdot 5^3}{2^5\cdot 7^2},\ \textit{if}\ \ \mu = -\tfrac{924}{5}.$$

$$\mathcal{L}_7^G: \quad \mathfrak{p} = \left(\tfrac{6}{245}\,\tfrac{(97\mu+1606)^2(87\mu^2+528\mu+2596)^2}{(1093\mu^3+49566\mu^2-838068\mu+1549769)^2},\ \tfrac{301158}{30625}\,\tfrac{(61\mu^2-44\mu-6556)^2(2021\mu^2+1496\mu-157476)}{(1093\mu^3+49566\mu^2-838068\mu+1549769)^2}\right)$$
$$\textit{and}\quad 8000000\,\mathfrak{p}^3 - 404568000\,\mathfrak{p}^2 - 31666132872\,\mathfrak{p} + 308290455 = 0,$$
$$\textit{if}\quad 1093\mu^3 + 49566\mu^2 - 838068\mu + 1549769) = 0.$$

$$\mathcal{L}_8^G: \quad \mathfrak{p} = \left(\tfrac{49}{11236320}\,\tfrac{(279\mu+15028)^2}{(7\mu+884)^2},\ \tfrac{1}{1360026486}\,\tfrac{\mu(3675\mu+3321188)^2}{(7\mu+884)^3}\right)$$
$$\textit{and}\quad \mathfrak{p} = \tfrac{2^3\cdot 3^{11}\cdot 101^4}{5^3\cdot 7^4\cdot 13^6},\ \textit{if}\ \ \mu = -\tfrac{884}{7}.$$

$$\mathcal{L}_9^G: \quad \mathfrak{p} = \left(\tfrac{605}{5633766}\,\tfrac{(9\mu-7200)^2}{(3\mu+836)^2},\ \tfrac{90}{370680937}\,\tfrac{\mu(157\mu+79420)^2}{(3\mu+836)^3}\right)$$
$$\textit{and}\quad \mathfrak{p} = -\tfrac{2^9\cdot 5\cdot 11^2}{3^7},\ \textit{if}\ \ \mu = -\tfrac{836}{3}.$$

$$\mathcal{L}_{10}^G: \quad \mathfrak{p} = \left(\tfrac{147}{90250}\,\tfrac{(181\mu+1598)^2\,(3813\mu^2+15912\mu-39236)^2}{(251\mu-782)^2\,(115\mu^2-68\mu-6596)^2},\ \tfrac{5007792000}{121}\,\tfrac{(7877\mu^2+3128\mu-374884)^2\,(115\mu^2-68\mu-6596)^2}{(251\mu-782)^2(181\mu+1598)^2\,(3813\mu^2+15912\mu-39236)^2}\right)$$
$$\textit{if}\quad (251\mu-782)\,(115\mu^2-68\mu-6596)\,(181\mu+1598)\,(3813\mu^2+15912\mu-39236) = 0$$
$$\textit{then}\quad \mathfrak{p} = -\tfrac{950367275}{21168\cdot Q}\cdot\tfrac{(402998158\mu^2-4363415636\mu+25170477\mu^3+13083554824)^4}{(1268277\mu^2-5261568\mu+18129548)^2\,(-287844+7959\mu^2-65756\mu)^2}\cdot \frac{1}{228384659961\mu^4-22196181318948\mu^3+185588379432544\mu^2-447275488903152\mu+658755318269936}$$

$$\mathcal{L}_{12}^G: \quad \mathfrak{p} = \left(\tfrac{1}{268203000}\,\tfrac{(6611\mu-501500)^2}{(11\mu+1700)^2},\ \tfrac{56}{284015801875}\,\tfrac{\mu\,(20933\mu-5686500)^2}{(11\mu+1700)^2}\right)$$
$$\textit{and}\ \mathfrak{p} = \tfrac{2\cdot 3^3\cdot 5\cdot 41^4}{7^4\cdot 11^2\cdot 17^2},\quad \textit{if}\ \ \mu = -\tfrac{1700}{11},$$

$$\mathcal{L}_4^G: \quad \mathfrak{p} = \tfrac{1764}{25}.$$

Proof. The proof of the theorem is computational. Let $\mathcal{X}_g$ be a hyperelliptic curve of $g \le 12$ with $\mathrm{Aut}(\mathcal{X}_g) \cong \mathbb{Z}_2 \oplus A_4$, or $SL_2(3)$. From Lemma 2.1. we have $g = 4, 5, 7, 8, 9, 10, 12$. If $g = 4$ then the curve is isomorphic to

$$Y^2 = X(3X^4 + 1)(3X^4 + 6X^2 - 1),$$

hence $\mathfrak{p}(\mathcal{X}_4) = \frac{1764}{25}$.

For other cases we compute $\mathfrak{p}$ where the equation of the curve is given as in Table 2. If $g = 5, 8, 9, 10, 12$, we substitute $\mu = \lambda^2$ and get expressions in (13). For $g = 7, 10$ we substitute $\mu := \lambda\sqrt{-3}$ and get $\mathfrak{p}$ is as in (13).

□

In each case one can find an equation for $\mathcal{L}_g^G$ by eliminating μ. Each nonsingular point $\mathfrak{p} \in \mathcal{L}_g^G$ correspond to a hyperelliptic curve $\mathcal{X}_g$ (up to isomorphism) with automorphism group G. One can show that singular points of $\mathcal{L}_g^G$ corresponds to hyperelliptic curves $\mathcal{X}_g$ such that G is a proper subgroup of $\mathrm{Aut}(\mathcal{X}_g)$.

Example 5.1. *Let* $g = 5$. *Then eliminating* μ *from equations of* $\mathcal{L}_G^5$ *we get*

$$4920750i_1^3 - 28224i_2^2 - 164025i_1^2 - 136080i_1i_2 + 672i_2 + 1620i_1 - 4 = 0 \tag{13}$$

There is only one singular point $\mathfrak{p} = \left(0, \frac{1}{84}\right) \in \mathcal{L}_G^5$. *The genus 5 curve corresponding to this point has equation*

$$Y^2 = X^{12} - \frac{484}{5}X^{10} - 33X^8 + \frac{968}{5}X^6 - 33X^4 - \frac{484}{5}X^2 + 1$$

One can show that this curve has automorphism group of order 48. It is the only genus 5 hyperelliptic curve (up to isomorphism) with automorphism group of order 48.

5.1. **Field of moduli versus field of definition.** Let $\mathcal{X}$ be a curve defined over k. The **field of moduli** of $\mathcal{X}$ is a subfield $F \subset k$ such that for every automorphism σ of k $\mathcal{X}$ is isomorphic to $\mathcal{X}^\sigma$ if and only if $\sigma_F = id$. The field of moduli is not necessary a field of definition.

In [11] we conjectured that the field of moduli is the field of definition for all hyperelliptic curves with extra automorphisms (i.e., automorphism group of order > 2). Moreover, it is a corollary of Theorem 4.2. in [11], that field of moduli is the field of definition for all hyperelliptic curves $\mathcal{X}_g$ which have more than 3 involutions. As a consequence this is the case for curves $\mathcal{X}$ with $\mathrm{Aut}(\mathcal{X}) \cong \mathbb{Z}_2 \oplus A_4$ (see Table 1 for the number of involutions). This is done in [11] via dihedral involutions. Since every curve with automorphism group $\mathbb{Z}_2 \oplus A_4$ has an extra involution then its equation can be written as

$$Y^2 = F(X^2).$$

Then the field of moduli is determined by the g-tuple of dihedral invariants $\mathfrak{u} = (\mathfrak{u}_1, \ldots, \mathfrak{u}_g)$. The reduced automorphism group of the curve has another involution if and only if

$$2^{g+1}u_1^2 - 4u_g^{g+1} = 0 \tag{14}$$

In this case we give an equation of the curve in terms of the dihedral invariants $\mathfrak{u}_1, \ldots, \mathfrak{u}_g$, see [11] for details. We illustrate this method with the case $g = 5$.

Example 5.2. *Let* $g = 5$ *and* $\mathcal{X}_5 \in \mathcal{L}_G^5$. *Then,*

$$Y^2 = X^{12} - \lambda X^{10} - 33X^8 + 2\lambda X^6 - 33X^4 - \lambda X^2 + 1$$

Dihedral invariants of this curve are:

$$u_1 = 2\lambda^6, u_2 = -66\lambda^4, u_3 = -4\lambda^4, u_4 = -66\lambda^2, u_5 = 2\lambda^2,$$

see (10) for their definitions with $n = 2$. *It can be easily checked that (14) holds. Hence, the field of moduli is the same as the field of definition from results in [11].*

Let $\mathcal{X}$ be a curve which belongs to one of the spaces in (13). Then the field of moduli is determined by $\mathfrak{p}(\mathcal{X}) = (\mathfrak{p}_1, \mathfrak{p}_2)$. The field of moduli is a field of definition if one can find a curve $\mathcal{Y}$ isomorphic to $\mathcal{X}$ and with coefficients given as rational functions in $\mathfrak{p}_1, \mathfrak{p}_2$.

Proposition 5.1. *Let* $\mathfrak{p} \in \mathcal{L}_g^G$ *and* μ *the parameter of Theorem (5.1.). Then,* $\mathcal{X}_g$ *such that* $\mathfrak{p} = [\mathcal{X}_g]$ *is isomorphic to*

$$
\begin{aligned}
\mathcal{X}_5: \quad & Y^2 = M(X), \\
\mathcal{X}_7: \quad & Y^2 = (3X^4 + 6X^2 - 1) \\
& \qquad (27X^{12} - 27\mu X^{10} + 297X^8 - 18X^6 - 99X^4 + 3\mu X^2 + 1), \\
\mathcal{X}_8: \quad & Y^2 = X(\mu X^4 - 1)\, M(X) \\
\mathcal{X}_9: \quad & Y^2 = (\mu^2 X^8 + 14\mu X^4 + 1)\, M(X), \\
\mathcal{X}_{10}: \quad & Y^2 = X(3X^4 + 1)(3X^4 + 6X^2 - 1) \\
& \qquad (27X^{12} - 27\mu X^{10} + 297X^8 - 18X^6 - 99X^4 + 3\mu X^2 + 1), \\
\mathcal{X}_{12}: \quad & Y^2 = X(\mu X^4 - 1)(\mu^2 X^8 + \mu X + 1)\, M(X),
\end{aligned} \tag{15}
$$

where $M(X) := \mu^3 X^{12} - \mu^3 X^{10} - 33\,\mu^2 X^8 + 2\,\mu^2 X^6 - 33\,\mu X^4 - \mu X^2 + 1$.

Proof. For the computationally minded reader, simply compute the invariants in each case. These invariants are the same as given in (13). Thus, the curve corresponds to $\mathfrak{p}$. However, it is important to know explicitly the isomorphism between curves in (13) and curves in (15).

Fix $\mathfrak{p} \in \mathcal{L}_g$ as in (13). Let $g = 5, 8, 9, 12$. Then the curve $\mathcal{X}_g$ given in Table 2 corresponds to $\mathfrak{p}$ (in all cases) since that is how we computed $\mathfrak{p}$. Let $X = \sqrt{\lambda}\, X$ and $\mu = \lambda^2$ and we get equations as in (15). Since, $\mu = \lambda^2$ in all these cases of Theorem 5.1., then the proof is complete.

Let $g = 7$. The equation of the curve is

$$Y^2 = (X^4 + 2\sqrt{-3}X^2 + 1)G_1(X)$$

Let $\mu := \lambda\sqrt{-3}$ and perform the transformation $X \to (-3)^{\frac{1}{4}}X$. Hence, the curve is isomorphic to $\mathcal{X}_7$ in (15). The case $g = 10$ goes the same way as $g = 7$. □

Proposition 5.2. *Let $\mathcal{X}$ be a hyperelliptic curve of genus $g \leq 12$ such that $\overline{Aut}(\mathcal{X}) \cong A_4$. Then, the field of definition of $\mathcal{X}$ is the same as the field of moduli. Moreover, the equation of the curve in terms of its invariants is given in (15).*

Proof. In each case of (13) it is easily shown that μ is a generator of $k(\mathfrak{p}_1, \mathfrak{p}_2)$ (i.e., μ can be expressed as a rational function in terms of $\mathfrak{p}_1, \mathfrak{p}_2$).

□

There is no particular reason why we focused on $g \leq 12$. Indeed the same technique can be used for higher genus. However, there is no obvious way to generalize Proposition 5.2. to any genus g in the case when the group is $SL_2(3)$.

References

[1] R. Brandt and H. Stichtenoth, Die Automorphismengruppen hyperelliptischer Kurven, *Man. Math* **55** (1986), 83–92.

[2] E. Bujalance, J. Gamboa, and G. Gromadzki, The full automorphism groups of hyperelliptic Riemann surfaces, *Manuscripta Math.* **79** (1993), no. 3-4, 267–282.

[3] M. Fried and H. Völklein, The inverse Galois problem and rational points on moduli spaces. Math. Ann. 290 (1991), no. 4, 771–800.

[4] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.2; 2000. (`http://www.gap-system.org`)

[5] J. Gutierrez and T. Shaska, Hyperelliptic curves with extra involutions, 2002 (submitted).

[6] J. Igusa, Arithmetic variety of moduli for genus two. Ann. of Math. (2) 72 1960 612–649.

[7] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, The locus of curves with prescribed automorphism group, *RIMS Kyoto Series*, Communications in Arithmetic Fundamental Groups, ed. H. Nakamura, 2002, 112-141.
[8] H. Niederreiter, C. Xing, Rational points on curves over finite fields: theory and applications. London Mathematical Society Lecture Note Series, 285. Cambridge University Press, Cambridge, 2001.
[9] T. Shaska, Curves of genus 2 with (n, n) decomposable Jacobians, *J. Symbolic Comput.*, 31 (2001), no. 5, 603–617.
[10] T. Shaska, Genus 2 curves with degree 3 elliptic subcovers, *Forum Math.*, 2002, (accepted).
[11] T. Shaska, Computational aspects of hyperelliptic curves, The Sixth Asian Symposium on Computer Mathematics (Beijing, 2003), Lect. Not. Ser. on Comp., World Scientific Publ., Singapore/River Edge, USA, 2003.
[12] T. Shaska, Determining the automorphism group of hyperelliptic curves, *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, ACM, 2003.
[13] T. Shaska, Subvarieties of the moduli space of hyperelliptic curves, (in preparation).
[14] T. Shaska and H. Völklein, Elliptic subfields and automorphisms of genus two fields, *Algebra, Arithmetic and Geometry with Applications. Papers from Shreeram S. Abhyankar's 70th Birthday Conference*, Springer (2003).

Department of Mathematics,, University of Idaho, E-mail: tshaska@uidaho.edu